Welkom!
Webinar IT 2, Nen7510, CER en NIS2

4 juni 2024 – 15.30 – 16.30 uur

Werken aan IT 2, Nen7510, CER en NIS2

Het programma:

15.30	Welkom
15.35	Uitleg NIS2 • stand van zaken/tijdlijn • inhoud • verplichtingen • relatie met NEN 7510 • relevante instanties
15.50	Enkele stellingen
16.00	Korte uitleg: aanpak NIS2 bij ZZG zorggroep
16.10	Aanpak NIS2 in Netwerk Nonna Nijmegen
	Vragen

De sprekers van vandaag:

Leendert Buijtendijk
ICT manager en Security Officer
ZZG Zorggroep

Bart van den Heuvel
procesondersteuner
NONNA Netwerk

Opzet van dit webinar:

- Bedoeling van de webinars: (Actiz/VGN) leden ondersteunen elkaar. Wij zijn geen beveiligingsprofessionals.
- De presentatie bevat veel informatie en links, met de bedoeling om je op weg te helpen - niet alles zal uitgebreid worden behandeld maar de presentatie wordt gedeeld. De laatste sheet bevat voornamelijk verwijzingen (links) naar meer (detail) informatie over NIS2.

Tijdlijn

- 2 Richtlijnen (eind 2022 aangenomen door EU):
  - CER: Critical Entities Resilience Directive
    - Gaat over Fysieke weerbaarheid. Bescherming van organisaties tegen fysieke dreigingen, zoals de gevolgen van (terroristische) misdrijven, sabotage en natuurrampen
    - Zal worden uitgewerkt in Wet weerbaarheid kritieke entiteiten (Wwke)
    - Hier vermeld omdat implementatie parallel loopt, maar in principe gescheiden is van NIS
  - NIS2 (NL naam NIB2): Network en Information Security Directive
    - Digitale weerbaarheid
    - NIS2 is opvolger van NIS (In Nederland NIB genoemd).
    - NIB is in NL uitgewerkt in de Wbni (Wet beveiliging netwerk en informatiesystemen) uit Nov 2018. Deze geldt voor essentiële diensten, die per Amvb/besluit worden bepaald. In het Bbni (Besluit beveiliging netwerk- en informatiesystemen) was gezondheidszorg niet als essentiële sector aangewezen.
  - Bij NIS2 is in de Richtlijn al bepaald wat essentiële diensten/sectoren zijn, en daar zit gezondheidszorg volledig bij.
  - De NIS2 Richtlijn is geen wet maar draagt EU-lidstaten op welke zaken zij in wetten dienen te regelen.
  - Naar verwachting wordt de wetgeving in NL van kracht vanaf 2025
    - Huidige Wbni, Wet beveiliging netwerk- en informatiesystemen, wordt ingetrokken
    - Wordt vervangen door ‘Cyberbeveiligingswet’
  - Internetconsultatie staat vanaf 21/5/2024 open (tot 1/7/2024)
    - www.internetconsultatie.nl/cyberbeveiligingswet
    - Wetsvoorstel (consultatieversie)
    - Memorie van Toelichting
    - Goed leesbaar !

Welke organisaties vallen onder NIS2

- Sectoren die zijn genoemd in de bijlagen van de richtlijn
  - Dat is het geval voor gezondheidszorg
  - Alle zorgaanbieders vallen hieronder
- En organisatie is een ‘belangrijke’ of ‘essentiële entiteit

Essentieel als

- Grote entiteit genoemd in bijlage 1 (gezondheidszorg valt hieronder)
- En ‘groot’ is dan
  - Minimaal 250 werknemers
  - En/Of (dit is nog niet bepaald!) > 50 mln omzet en balanstotaal > 43 mln

Belangrijk als

- Genoemd in bijlage 1 en middelgroot (minstens 50 werknemers of jaaromzet of balanstotaal boven 10 mln

Een gezondheidszorgorganisatie valt dus altijd onder NIS2 maar kan Essentieel of Belangrijk zijn.

Dit heeft gevolgen voor de verplichtingen waaraan moet worden voldaan.

Verplichtingen (1/2)

Zorgplicht

- Uitvoeren van een risicobeoordeling en passende maatregelen nemen
- Dit komt sterk overeen met verplichtingen obv NEN 7510

Toezicht

- Essentiële entiteiten: toezicht ‘vooraf’ (ex ante) (art 32-34 richtlijn)
  - maatregelen documenteren + op verzoek overleggen aan bevoegde autoriteit
    - Niet alleen ‘opzet en bestaan’ maar ook ‘werking’ kunnen aantonen
  - eventueel onafhankelijke audits, al dan niet aangekondigd
  - beveiligingsscans
  - kosten in principe voor de ‘gecontroleerde entiteit’ tenzij anders geregeld
  - Audits kunnen leiden tot
    - waarschuwingen
    - bindende aanwijzingen (opdrachten) om zaken te doen of juist te laten evt met termijnen
  - Boetes i.v.m. handhaving, minimaal 10 mln of 2% van de wereldwijde jaaromzet

- Belangrijke entiteiten
  - Toezicht vergelijkbaar met Essentiele entiteiten, echter in principe alleen achteraf (ex post)
  - Als er bewijs, aanwijzing of informatie is dat zij hun verplichtingen t.a.v. NIS2 schenden
  - Boetes i.v.m. handhaving minimaal 7 mln of 1,4% wereldwijde jaaromzet

Verplichtingen (2/2)

Meldplicht / Informatieplicht / Registratieplicht

- Incidenten moeten gemeld worden
  - Incident is een gebeurtenis die de beschikbaarheid, betrouwbaarheid of vertrouwelijkheid in gevaar brengt van diensten die worden aangeboden door of toegankelijk zijn via netwerk en informatiesystemen.
- Melden moet bij bevoegde autoriteit, bepaald door Min. voor Medische Zorg en Sport
  - en/of bij zijn Computer Security Incident Response Teasm (CSIRT). Levert hulp en bijstand. In NL is dat op grond van de huidige Wbni het NSC (Nationaal Cyber Security Centrum)
- Melden als de dienst aanzienlijk verstoord wordt. O.a. afh van aantal betrokken personen, duur van de verstoring en fin. gevolgen
- Melden bestaat uit 4 fasen:
  - Binnen 24 uur een eerste melding
  - Binnen 72 uur een uitgebreidere melding
  - Een tussentijds verslag op verzoek CSIRT
  - Binnen maand na optreden een gedetailleerd eindverslag

NIS2 en NEN 7510

- Wie compliant is met NEN 7510 zal al aan veel zo niet alle zaken die vallen onder de Zorgplicht voldoen, zoals
  - Risico analyse
  - Een ISMS
  - Continuïteitsplannen
  - Bewustwording medewerkers

    NB voor Actiz leden: Routekaart informatieveiligheid / NEN 7510
- NIS2 voegt vooral toe:
  - Meldings-, Informatie- en Registratieplicht
    - Aan instanties en informeren betrokkenen bij security incidenten
  - Bestuurdersverantwoordelijkheid voor informatiesecurity (NB NEN 7510 vraagt ook al nadrukkelijk om bestuurdersparticipatie).

(Zeer) beknopte inhoud van de Richtlijn

Om te zetten in wetgeving; zie inmiddels ook consultatieversie wetsvoorstel

- Bepalen belangrijke / essentiële entiteiten
- Nationale cyberbeveiligingsstrategie vaststellen (art 7)
- Bevoegde autoriteiten aanwijzen voor o.m. monitoring (art 8)
- Aanstellen autoriteit(en) voor beheer grootschalige cyber incidenten + nationaal plan hiervoor (art 9)
- Instellen 1 of meer CSIRT (Computer Security Incident Response Team), verantwoordelijk voor incidentbehandeling (art 10, 11)
- Via (een) CSIRT gecoördineerd bekend maken van kwetsbaarheden
- Samenwerking op internationaal niveau (art 14, 15) oa via 'EU-CyCLONe' (art 16) =EU netwerk van verbindingsorganisaties voor cybercrises
- Inrichting collegiale toetsing tussen lidstaten (art 19)
- Bestuurders van essentiële entiteiten moeten opleiding volgen (en liefst ook medewerkers) om cyberrisico's te onderkennen en maatregelen beoordelen (art 20)
- Belangrijke/essentiële entiteiten moeten passende maatregelen treffen (art 21)
- Rapportageverplichting bij incidenten voor belangrijke/essentiële entiteiten (art 23)
- Lidstaten kunnen certificering afdwingen van ICT producten of diensten (art 24)
- Een betrouwbaar register voeren van relevante entiteiten zoals DNS-dienstverleners, domein registrars enz. (art 27, 28)
- Zorgen dat de Entiteiten vrijwillig informatie terzake cyber security kunnen delen (art 29)
- Zorgen voor effectief toezicht op handhaving van de richtlijn (prioritering obv risico mag) (art 31, 32, 33)
- Opleggen van boetes als onderdeel van handhaving met minimum hoogtes (art 34)
- Meldingen mbt inbreuken wat betreft persoonsgegevens blijven onverkort gelden (art 35)
- Lidstaten staan elkaar bij als dienstverlening of ICT systemen zich over meerdere lidstaten verdelen (art 37)
- Uiterlijk 17 oktober 2024 stellen lidstaten de bepalingen vast om aan de richtlijn te voldoen. (art 41)

Betrokken / relevante instanties I

Toezichthouder

- IGJ
  - Na aanpassing Wbni in oktober 2024 wordt toezichthouder in ‘lagere’ wetgeving aangewezen
  - Inspectie Gezondheidszorg en jeugd, IGJ, krijgt deze rol
  - Zie ook toetsingskader IGJ Digitale Zorg (verwijst momenteel naar o.a. NEN 7510 nog niet naar NIS2)
- Z-Cert
  - Voor AED’s (Aanbieders van essentiële diensten) is het Nationaal Cyber Security Centrum (NCSC) op grond van Wbni het CSIRT
  - Hier (AED) viel Gezondheidszorg nog niet onder. (Mede) daarom is in 2018 Z-Cert opgericht als stichting door o.a. NVZ, Universitaire ziekenhuizen, GGZ Nederland en het NCSC.
  - Z-CERT biedt zorginstellingen specifieke en gespecialiseerde diensten om de weerbaarheid ten aanzien van cybersecurity te vergroten, en ondersteunt op het moment dat een zorginstelling door een incident wordt getroffen
  - Z-CERT is (nu) voor NCSC een schakelorganisatie voor doorgeven info tav cyber beveiliging en dient ondersteuning te bieden om schade te beperken en dienstverlening zsm te kunnen hervatten
  - In de nieuwe wet fungeert NCSC in het algemeen als CSIRT functioneert maar er kunnen ook aparte CSIRT’s voor bepaalde sectoren aangewezen worden.
  - Verwacht wordt dat Z-CERT aangewezen wordt als CSIRT tbv de zorgsector.

Taken van een CSIRT

- het **monitoren en analyseren** van cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau, en, op verzoek, het verlenen van bijstand aan betrokken essentiële en belangrijke entiteiten met betrekking tot het realtime of bijna-realtime monitoren van hun netwerk en informatiesystemen;
- het **verstrekken van vroegtijdige waarschuwingen**, meldingen en aankondigingen en het verspreiden van informatie onder betrokken essentiële en belangrijke entiteiten en aan de bevoegde autoriteiten en andere relevante belanghebbenden over cyberdreigingen, kwetsbaarheden en incidenten, in bijna-realtime indien mogelijk;
- het **reageren op incidenten en verlenen van bijstand** aan de betrokken essentiële en belangrijke entiteiten, indien van toepassing;
- het verzamelen en analyseren van forensische gegevens en het zorgen voor dynamische risico- en incidentenanalyse en situationeel bewustzijn met betrekking tot cyberbeveiliging;
- op verzoek van een essentiële of belangrijke entiteit: het proactief scannen van de netwerk- en informatiesystemen van de betrokken entiteit om kwetsbaarheden met mogelijk significante gevolgen op te sporen;
- het deelnemen aan het CSIRT-netwerk en, in overeenstemming met hun capaciteiten en bevoegdheden, het verlenen van wederzijdse bijstand aan andere leden van het netwerk op hun verzoek;
- indien van toepassing, het optreden als coördinator ten behoeve van het in artikel 12, lid 1 bedoelde proces van gecoördineerde bekendmaking van kwetsbaarheden;
- het bijdragen aan de uitrol van veilige instrumenten voor het delen van informatie op grond van artikel 10, lid 3.

Betrokken / relevantie instanties II

Nationaal Cyber Security Center (NCSC)

- een onderdeel van het ministerie van Justitie en Veiligheid, heeft als taak om organisaties te waarschuwen als er in de software die zij gebruiken een kwetsbaarheid is ontdekt en ze kunnen worden gehackt. Het NCSC richt zich vooral op de organisaties van de rijksoverheid en op sectoren die als ‘vitaal’ zijn aangewezen, zoals energie, vervoer en drinkwater, internet en financieel betalingsverkeer.
- Het NCSC kan overheidsorganisaties en bedrijven dreigingsinformatie sturen. Voor een deel gaat dat rechtstreeks, voor een ander deel gaat het via zogenaamde schakelorganisaties, die ieder vanuit een bepaalde sector zijn opgezet. Zulke schakelorganisaties zijn er op dit moment voor de gemeenten, de zorg en het onderwijs, voor internetproviders en bedrijven in de hightech- en maakindustrie, maar ook voor de Rotterdamse haven

Betrokken / relevantie instanties III

Digital Trust Center

- Het ministerie van Economische Zaken en Klimaat (EZK) heeft in 2018 het Digital Trust Center (DTC) opgericht. Dit is gericht op bedrijfsleven. Het DTC heeft als missie om ruim 2 miljoen Nederlandse bedrijven weerbaarder te maken tegen toenemende cyberdreigingen. Alles van zzp'ers tot en met het grootbedrijf. Dit zijn alle bedrijven in Nederland die tot de niet-vitale sectoren behoren. Vitale sectoren, zoals banken, telecom-, energie-, en waterbedrijven, hebben het Nationaal Cyber Security Centrum (NCSC) als samenwerkingspartner binnen de Rijksoverheid.
- Z-CERT en het Digital Trust Center (DTC) bundelen de krachten op het gebied van cyberweerbaarheid van de zorgsector. Z-CERT mag gebruikmaken van de door DTC ontwikkelde adviezen en producten en zal deze zorg-specifieker aanbieden op zijn website en aan zijn deelnemers. Er zal regelmatig overleg plaatsvinden tussen het DTC en Z-CERT.https://www.digitaltrustcenter.nl/samenwerkingsverband/z-cert

Betrokken / relevantie instanties IV

ENISA, Agentschap van de Europese Unie voor Cyberbeveiliging

- Het Agentschap werkt samen met organisaties en bedrijven om het vertrouwen in de digitale economie te versterken, de veerkracht van de infrastructuur van de EU te vergroten en uiteindelijk de digitale veiligheid van de EU-burgers te waarborgen. Dit gebeurt door kennis te delen, personeel en structuren te ontwikkelen en voorlichting. De cyberbeveiligingsverordening van de EU heeft het werk van het agentschap versterkt.

- Enisa werkt voornamelijk ten behoeve van overheidsinstanties:
  - autoriteiten, instellingen en gedecentraliseerde organen en agentschappen in de EU-landen
  - EU-instellingen, -agentschappen en -organen
- Het agentschap helpt ook:
  - de IT-sector (telecommunicatie, internetaanbieders en IT-bedrijven)
  - het bedrijfsleven — met name kleine en middelgrote ondernemingen
  - deskundigen op het gebied van cyberbeveiliging (bv. cybersecurity incident response teams)
  - de academische wereld
  - het grote publiek

https://www.enisa.europa.eu/

Stelling 1

Wij gaan pas serieus aandacht besteden aan (voldoen aan) NIS2 als de wetgeving er is (in 2025)

- Eens
- Oneens

Stelling 2

Wij denken uiterlijk Q2 van 2025 wel te kunnen voldoen aan NIS2

- Nee
- Misschien gedeeltelijk
- Voor het grootste deel wel
- Helemaal

Stelling 3

Hoe pakken we NIS2 aan

- Wij kunnen zelfstandig voldoen aan NIS2
- Wij huren hiervoor externen in
- Wij doen dit samen met collega instellingen
- Externen + met collega instellingen

Stelling 4

De NIS2 gaat grote impact hebben op de informatie- en netwerkbeveiliging in onze organisatie

- Ja zeker
- Er verandert wel wat, maar niet overwegend
- Nee niet of nauwelijks

Stelling 5

Wij zijn al NEN 7510 compliant (of gecertificeerd)

- Nee, we moeten eigenlijk nog starten
- Begonnen, maar nog lang niet klaar
- Nog niet, maar goed op weg
- Jazeker !

Aanpak Cybersecurity bij ZZG zorggroep

Organisatie:

- SeCo (security officer) - (Nog) gecombineerd met manager IT
- Coördinatie team InformatieVeiligheid
- Rollen belegd bij anderen conform informatiebeveiligingsbeleid:
  - Managers
  - Gebruikers
  - Applicatie eigenaren
  - Functioneel beheerders

Aanpak Cybersecurity bij ZZG zorggroep

Acties:

- NEN 7510 implementeren
  - Informatiebeveiligingsbeleid, risico analyse, ISMS zijn beschreven en (net) formeel vastgesteld
  - ‘PDCA’ cyclus gaat nu starten
- Aandacht en betrokkenheid vanuit RvB is er
- Regelgeving NIS2 goed volgen
- Helderheid krijgen over wat vanuit Z-Cert (als CSIRT) geregeld gaat worden en welke ondersteuning zij gaan bieden
- Aanvullende risico analyse NIS2 maken (wat moeten we nog regelen)
- Waarschijnlijk gaat NIS2 extra aandacht vragen voor:
  - Leveranciersmanagement (Cloud applicaties en netwerkbeheer)
  - Intern calamiteiten respons team en procedures (ook droog oefenen)
  - Onderzoek naar verzekering / extra ondersteuning
  - Procedures voorbereiden voor rapportage (analoog aan meldingen privacy incidenten o.b.v. AVG)

Aanpak Cybersecurity in netwerk NONNA

NONNA
(Netwerknonna.nl)

- Bundeling van 14 organisaties in de ouderenzorg in regio Nijmegen
- Samenwerking op thema's
  - Wonen
  - Werken
  - Slim samen
    - Bv Avond/Nacht en weekendzorg of Crisisregeling
    - Maar ook IT en Zorgtechnologie
      - **Werkgroep Samenwerking Cybersecurity Nonna**

Voor nu en later

Aanpak Cybersecurity in netwerk NONNA

Doelstellingen Werkgroep Cybersecurity Nonna

- Aantoonbaar voldoen (minimale) wet- en regelgeving, maar vooral ook:
- Cybersecurity bewuste medewerkers
- Beproefd veilige en proactief ingerichte digitale werkomgeving
- Voorbereid zijn op mogelijke calamiteit/hack en hierop kunnen acteren (incident response)

Samenwerking:

- Kennisdeling en menskracht van elkaar gebruiken
- Inkoopkracht
- Goede partner zijn voor elkaar en externe partijen

Voor nu en later

Aanpak Cybersecurity in netwerk NONNA

Scope voor Cybersecurity: IVDO

- Inrichten
  - Waar moet de organisatie aan voldoen, en wat is daarvoor nodig
  - NEN 7510 benadering
- Voorkomen
  - Welke acties zijn nodig om weerbaarder te worden, aan wet en regelgeving te voldoen en aansprakelijkheid te mitigeren (organisatie mens en techniek)
- Detecteren
  - Hoe ervoor zorgen dat je weet als/wanneer er iets aan de hand is
- Oplossen
  - Wat, hoe en bij wie ontdekken van een incident en het oplossen van de problemen

Voor nu en later

Aanpak Cybersecurity in netwerk NONNA

Samenwerking op het gebied van onder andere

- Inzet van capaciteit, denk aan:
  - samen inhuren van CISO
- Inregelen NEN 7510 / ISMS
- Uitvoeren van een bewustwording / Awareness programma
- Beschikbaarheid Incident Response Team
- Verzekering

Voor nu en later

Verdere informatiebronnen NIS2

- Vragen en antwoorden over de richtlijn Netwerk en Informatiebeveiliging (NIS2): https://z-cert.nl/vragen-en-antwoorden-over-de-richtlijn-netwerk-en-informatiebeveiliging-nis2/
- Nationaal coördinator Terrorismebestrijding en Veiligheid: www.nctv.nl
- Op de sites van het Z-CERT, het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center staan bijvoorbeeld een aantal maatregelen die organisaties kunnen implementeren om zich beter te beschermen tegen risico's en schade door cyberaanvallen. En op de website gegevensuitwisselingindezorg.nl van VWS is meer informatie te vinden onder het kopje Fysieke en digitale weerbaarheid.
- Bron: https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen
- https://www.gegevensuitwisselingindezorg.nl/weerbaarheid/tijdlijn
- https://rechtindezorg.nl/2023/07/03/cybersecurity-in-de-zorg-nieuwe-richtlijn-nis2/
- https://z-cert.nl/vragen-en-antwoorden-over-de-richtlijn-netwerk-en-informatiebeveiliging-nis2/
- Actiz routekaart informatieveiligheid ('Nen 7510') https://www.actiz.nl/mijn-actiz/landingspagina-routekaart-implementatie-informatiebeveiliging
- CER richtlijng (NL vertaling): https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32022L2557&from=EN
- Toetsingskader IGJ voor Digitale Zorg: https://www.igj.nl/publicaties/toetsingskaders/2024/05/06/toetsingskader-digitale-zorg-uitgebreide-versie
- https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/wie-doet-wat/csirts

Kijk voor meer informatie ook op deze websites:

- De volledige tekst van de NIS2-richtlijn: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32022L2555&qid=1678274777536
- De factsheet van de Europese Commissie over de NIS2
- Informatie vanuit VWS op gegevensuitwisselingindezorg.nl
- rijksoverheid.nl
- https://www.gegevensuitwisselingindezorg.nl/weerbaarheid

Vragen?

Dank voor uw deelname!

Meer informatie?

Contactpersonen:

- l.buijtendijk@zzgzorggroep.nl
- bart@wijtz.nu

Dit webinar is terug te kijken via: https://www.actiz.nl/mijn-actiz/webinars-terugkijken